BRIEFING

Requested by the INTA committee

European Parliament

Dual-use and cyber-surveillance: EU policies and current practices

Authors:

Rudi Du Bois and Alexandre Tapia Reyes (Deloitte Belgium)

European Parliament Coordinator:

Policy Department for External Relations

Directorate General for External Policies of the Union

PE 754.439 – November 2023

EN

DIRECTORATE-GENERAL FOR EXTERNAL POLICIES
POLICY DEPARTMENT

European Parliament

BRIEFING

Dual-use and cyber-surveillance: EU policies and current practices

ABSTRACT

This briefing paper on dual-use and cyber-surveillance provides on overview of current EU export controls of dual-use items in general and cyber-surveillance items in particular, and what the approach is in countries such as the US, the UK and Japan. It explains the impact of the sanctions against Russia on the export of dual-use items and the use of cyber-surveillance in the conflict in the Ukraine.

The Dual-use Regulation 2021/821 has broadened the scope of export controls and defines a new category of dual-use items, namely 'cyber-surveillance items' which is incorporated in the list of dual-use items in Annex I of the Regulation. Furthermore, the Regulation introduces a catch-all clause which makes the export of cyber-surveillance items not listed in Annex I subject to export authorisation when intended for use in connection with internal repression and/or the commission of serious violations of human rights and international humanitarian law.

Regarding the sanctions against Russia, the EU had published 11 sanctions packages by mid-November 2023, including the prohibition of direct or indirect export to Russia of dual-use items listed in Annex I of the EU Dual-use Regulation. In addition, technologically advanced items as listed in Annex VII to the sanctions Regulation 833/2014 are also prohibited for export to Russia. The EU is cooperating with the US, the UK and other allies to align on the sanctions measures against Russia. There is less international alignment regarding export restrictions on semiconductor equipment and technology destined for China.

EP/EXPO/INTA/FWC/2019-01/LOT5/3/C/21
November 2023

EN

© European Union, 2023

Policy Department, Directorate-General for External Policies

AUTHOR(S)

- Rudi Du Bois, Senior Manager, Deloitte, Belgium
- Alexandre Tapia Reyes, Senior consultant, Deloitte, Belgium

PROJECT COORDINATOR (CONTRACTOR)

- Jonas Rasmussen, Copenhagen Economics

This paper was requested by the European Parliament's Committee on International Trade (INTA).

The content of this document is the sole responsibility of the authors, and any opinions expressed herein do not necessarily represent the official position of the European Parliament.

CONTACTS IN THE EUROPEAN PARLIAMENT

Coordination: Wolfgang IGLER, Policy Department for External Relations

Editorial assistant: Balázs REISS

Feedback is welcome. Please write to wolfgang.igler@europarl.europa.eu

To obtain copies, please send a request to poldep-expo@europarl.europa.eu

VERSION

English-language manuscript completed in October 2023.

COPYRIGHT

Brussels © European Union, 2023

Reproduction and translation for non-commercial purposes are authorised, provided the source is acknowledged and the European Parliament is given prior notice and sent a copy.

This paper will be published on the European Parliament's online database, 'Think Tank.

Table of contents

1 Overview on EU dual-use regime and international agreements

In the EU, the trade in dual-use items is regulated by the EU dual-use regime which contains a list of dual-use items which is not developed at EU level, but derived from the list of dual-use goods agreed upon in the Wassenaar Arrangement and from lists issued in the following multilateral non-proliferation regimes: the Australia Group (AG), the Nuclear Suppliers Group (NSG), the Missile Technology Control Regime (MTCR) and the Chemical Weapons Convention (CWC).

1.1 Existing EU rules

1.1.1 EU Dual-use Regulation

Regulation (EU) 2021/821 of 20 May 2021 of the European Parliament and of the Council[1] sets up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items. This EU Dual-use Regulation (hereinafter 'the Regulation') establishes a harmonised EU export control regime which is binding in its entirety and directly and equally applicable in all EU Member States.

The EU dual-use regime aims at controlling cross-border movements of dual-use items by establishing a licensing requirement for exports to third countries. Article 2(1) of the Regulation defines dual-use items as '*items, including software and technology, which can be used for both civil and military purposes, and includes items which can be used for the design, development, production or use of nuclear, chemical or biological weapons or their means of delivery, including all items which can be used for both non-explosive uses and assisting in any way in the manufacture of nuclear weapons or other nuclear explosive devices*'.

Annex I of the Regulation contains a list of dual-use items (see section 1.1.2) the export of which requires an authorisation.

Licensing requirements not only apply to exports of dual-use items, but also to transit movements in the EU, to re-exports and to items temporarily exported outside the EU for processing. The definitions of these terms align with those in Union Customs Code. Furthermore, the transfer or transmission of dual-use software or dual-use technology is subject to authorisation as well as brokering activities in third countries that involve dual-use items.

The party responsible for determining if there is a licensing requirement for its shipment and to apply for an export license is the 'exporter' which is broadly defined in article 2(3) in alignment with the Union Customs Code. License applications must be made to the competent authority in the Member State where the exporter is established. Various license types are available.

Although there is a licensing requirement for dual-use items listed in Annex I of the Regulation, exports of items not listed in Annex I may be also subject to authorisation if the exporter has been informed by the authorities or if he is 'aware' that the items concerned are for use in connection of weapons of mass development or for a military end-use in a country under arms embargo. This is the so-called catch-all provision which appears in articles 3(2), 4, 5, 9 or 10 of the Regulation. These articles also allow Member States to include additional items on their national control list and impose a licensing requirement for such items.

[1] Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items (recast). Last updated on 26/05/2023

1.1.2 The EU dual-use list

The list of dual-use items is in Annex I of the Regulation. This list contains 10 categories which are derived from the List of Dual-Use Goods agreed upon by the Wassenaar Arrangement and from lists issued by the following multilateral non-proliferation regimes: the Australia Group (AG), the Nuclear Suppliers Group (NSG), the Missile Technology Control Regime (MTCR) and the Chemical Weapons Convention (CWC).

This dual-use list is regularly updated in conformity with changes in the lists issued by the above multi-lateral export control regimes.

Annex IV of the Regulation contains a list of sensitive items, which, according to article 11(1) of the Regulation require an authorisation when transferred within the territory of the EU.

1.1.3 Cyber-surveillance items

Article 2(20) of the Regulation defines cyber-surveillance items as '*dual-use items specially designed to enable the covert surveillance of natural persons by monitoring, extracting, collecting or analysing data from information and telecommunication systems*'.

The export of cyber-surveillance items listed in Annex I of the Regulation is subject to authorisation pursuant to article 3(1). There is also a catch-all provision for cyber-surveillance items not listed in Annex I pursuant to articles 5(1) and 5(2) of the Regulation. Art. 5.2 requires that an exporter informs his authorities when he '*is aware, according to his due diligence findings, that his item(s) may be intended, in their entirety or in part, for use in connection with internal repression and/or the commission of serious violations of human rights and international humanitarian law*'.

Art. 5(3) states that Member States may adopt or maintain national legislation in that respect and must inform its national customs authorities, the other Member States and the Commission of rules and authorisations it has issued in that respect.

Cyber surveillance items are listed in category 4 (Computers) and category 5 (Telecommunications and Information Technology) of the list of Dual-use Goods in Annex I of the Regulation. Below are the relevant dual-use codes.

- 4A005, 4D004 and related controls under 4E001.a. and 4E001.c. – 'Intrusion software';
- 5A001.f – 'Telecommunication interception systems'
- 5A001.j – 'Internet surveillance systems'
- 5D001.e – 'Communication monitoring software'
- 5A004.a – 'Items used to perform cryptanalysis'
- 5A004.b., 5D002.a.3.b. and 5D002.c.3.b – 'Forensic/investigative tools'.

1.2 International agreements: the Wassenaar Arrangement

The Wassenaar Arrangement (WA)[2] on Export Controls for Conventional Arms and Dual-Use Goods and Technologies is an international export control regime that aims to promote transparency and greater responsibility in transfers of conventional weapons and sensitive dual-use goods and technologies, and by doing so contributing to regional and international security and stability. Currently, 42 states participate in the Wassenaar Arrangement including all EU Member States.

The WA seeks to control the transfer of certain goods and technologies that have a dual use, i.e. that could be used for both civilian and military applications. Controlled items are specified in the List of Dual-Use Goods and Technologies and in the Munitions List. The Wassenaar List of Dual-Use Goods and

[2] https://www.wassenaar.org/

Technologies includes cyber-surveillance items. The Wassenaar list is updated every year and the participating states commit to adopt this list.

1.3 Other international agreements

The following multilateral agreements and conventions seek to control the proliferation of items that can be used in the development, production and use of weapons of mass destruction. They have issued lists of relevant items which the EU incorporates in the EU Dual-use list in Annex I of the Regulation.

- The Australia Group (AG)
- The Nuclear Suppliers Group (NSG)
- The Missile Technology Control Regime (MTCR)
- The Chemical Weapons Convention (CWC)

The lists issued by these groups do not specifically address cyber-surveillance items.

2 Dual-use sensitivities arising from the Russian war of aggression into Ukraine

Following the invasion of the Crimea Region in Ukraine by Russian forces in 2014, the EU had issued sanctions Regulation (EC) 833/2014[3] (hereinafter the 'sanctions Regulation') which has been further amended in response to the Russian invasion of Ukrainian territory in February 2022. To date, the EU has issued 11 sanctions packages against Russia, the first on 23 February 2022 and the latest on 23 June 2023.

In addition, the EU has also issued Council Regulation (EU) 269/2014 which imposes financial sanctions on Russian governmental and private persons and entities.

2.1 Dual-use provisions in sanctions regulation 833/2014

Article 2 of Council Regulation (EU) No 833/2014 states that '*it shall be prohibited to sell, supply, transfer or export, directly or indirectly,* ***dual-use goods and technology,*** *whether or not originating in the Union, to any natural or legal person, entity or body in Russia or for use in Russia*'.

Although not explicitly stated in this article, the dual-use goods and technology in scope are those listed in Annex I of EU Dual-use Regulation 2021/833.

- It must be noted that both sanctions Regulation 833/2014 and Dual-use Regulation 2021/821 apply in respect of exports to Russia. Where the Dual-use Regulation allows in principle exports of dual-use items, the sanctions Regulation against Russia explicitly prohibits exports of dual-use items to Russia and this provision prevails over the one of the Dual-use Regulation.
- Another scenario is that the sanctions Regulation allows for some derogations or exemptions but usually subject to authorization. In such case, two export licenses may be required: one under the sanctions Regulation and one under the Dual-use Regulation.

The prohibition in sanctions Regulation 833/2014 applies to goods, software, technology and also to the provision of technical assistance, brokering services, engineering and financial services related to the dual-use goods, software and technology. Its scope is therefore wider than that of the Dual-use Regulation.

Pursuant to **article 2a** of the sanctions Regulation, sales, supplies, transfers or exports, directly or indirectly, of goods and technology which might contribute to Russia's military and technological enhancement, or

[3] Council Regulation (EC) 833/2014 of 31 July 2024 concerning restrictive measures in view of Russia's actions destabilizing the situation in the Ukraine

the development of the defence and security sector, shall be prohibited if addressed to any natural or legal person, entity or body in Russia or for use in Russia.

Article 2a targets so-called **'advanced technology items'** which are listed **in Annex VII** to the sanctions Regulation. Annex VII has two parts. Part A contains a list of items (hardware, software and technology), grouped in nine categories, which are in most cases also specified in the dual-use list but with more stringent control parameters. Part B lists semiconductor devices, ICs, photographic cameras and other advanced equipment.

There are some exceptions to the prohibition in article 2a of the sanctions Regulation and their use is subject to government authorization. FAQ 18 in Part D published by the Commission[4] explains that'*For authorisations for goods and technology listed in Annex VII of the Sanctions Regulation, the rules and procedures laid down in the EU Dual-use Regulation apply, mutatis mutandis*'.

2.2 Impact on cyber-surveillance items

Export to Russia of cyber-surveillance items listed in Annex VII of the sanctions Regulation or on the dual-use list is prohibited. In the latest, 11th sanctions package their transit via the territory of Russia is also prohibited.

An exception to the prohibition is possible for certain cyber-surveillance items that are either on the dual-use list or in Annex VII subject to authorization.
Article 2a, paragraph 4 and 4(h) state that '*the competent authorities may authorise the sale, supply, transfer or export of the goods and technology referred to in paragraph 1 or the provision of related technical or financial assistance, for non-military use and for a non-military end-user, after having determined that such goods or technology or the related technical or financial assistance are*' (…) '(h) *intended for ensuring cyber-security and information security for natural and legal persons, entities and bodies in Russia except for its government and undertakings directly or indirectly controlled by that government*'.

According to FAQ D.2(17) national licensing authorities may issue not only individual but also global export licenses, covering multiple (civil) recipients. FAQ D.2(18) states that these licenses may cover subsequent updates such as bug fixes, malware fingerprint data) and/or upgrades (unlocking additional functionalities). The sanctions Regulation gives Member States some latitude in assessing whether or not to grant an exception and under what conditions.

3 EU position and reactions

In the age of digital revolution, cyber-surveillance technologies have become increasingly influential tools that, depending on their application, can either protect citizens or threaten the democratic ethos of societies. Recognizing the profound implications of these technologies, the European Union (EU) has taken decisive measures to ensure that their exports do not result in human rights violations or the undermining of democratic tenets. These measures not only emphasize the EU's unwavering commitment to defend human rights and democracy but also challenge other international actors to adopt a similarly robust stance.

[4] FAQ D.2(17) of the Commission Consolidated FAQs on the implementation of Council Regulation No. 833/2014 and Council Regulation no. 269/2014

3.1 Impact of the recast Dual-use Regulation 2021/821

- **The catch-all provision in article 5 of the Regulation[5]:** By providing the possibility to also control cyber-surveillance items not listed in Annex I of the Regulation, legislators are now able to keep up with emerging technologies and new developments in the area of cyber-surveillance.
- **Imposing due diligence:** The requirement for exporters to engage in due diligence transcends mere regulatory compliance. It fosters a culture of introspection, pushing companies to consider the ethical implications of their products. By gauging the potential for their technologies to be used for internal repression or to commit severe human rights violations, exporters become integral partners in upholding global democratic ideals[6].
- **A System of Accountability through Mandatory Notification:** The duty to notify competent authorities when exporters 'are aware' of potential misuse fosters a cooperative synergy between industry players and regulatory bodies. It not only ensures real-time regulatory compliance but also positions exporters as vigilant custodians of ethical tech exports.

3.2 Complementing the regulation: holistic EU initiatives

The Dual-use Regulation, while foundational, is complemented by a suite of EU strategies that provide a holistic solution:

- **European Cybercrime Centre (EC3):** With the EC3 at the helm, the EU's fight against cybercrime, especially misuse of surveillance systems and technology, becomes coherent and unified. This concentrated effort fortifies the EU's cyber-defences and ensures a coordinated response to emerging threats[7].
- **A Guiding Code of Conduct:** Crafting a code of conduct serves dual purposes. It offers exporters a clearer framework for ethical operations and enshrines the EU's expectations for responsible behavior. This code becomes a touchstone for ethical business operations, further entrenching a culture of responsibility[8].
- **Championing Human Rights and Democracy Abroad:** The EU's initiatives, aimed at bolstering human rights and democracy in vulnerable regions, reflect its commitment to preemptive solutions. By fortifying democratic infrastructures globally, the EU aims to reduce the allure of repressive cyber-surveillance in the first place[9].

3.3 Broader implications of the EU approach

The approach adopted by the EU in respect of cyber-surveillance and cyberware has the following implications.

- **Balancing potential conflicting interests and provide clarity and accountability:** By offering definitive guidelines through the Dual-use Regulation, the EU streamlines the compliance process for exporters. It removes ambiguities and establishes a clear pathway for ethical exports. This

[5] EU Dual-use Regulation (EU) 2021/821
[6] Guidelines on the Export of Cyber-Surveillance Items under Article 5 of Regulation (EU) No 2021/821 (Directorate-General for Trade, March 31, 2023).
[7] European Cybercrime Centre – EC3 | Europol, Europol, n.d., https://www.europol.europa.eu/about-europol/european-cyber-crime-centre-ec3.
[8] Ibid
[9] Human Rights & Democracy | EEAS, n.d., https://www.eeas.europa.eu/eeas/human-rights-democracy_en.; see, Council Conclusions on the EU Action Plan on Human Rights and Democracy 2020-2024 of November 2021, 12848/20

initiative not only eradicates ambiguities but also lays down a precise framework that champions ethical export practices.

- **Proactivity:** Beyond restrictive measures, the European Union's approach to export control also embraces proactivity. This is evident in their initiatives to support countries that are susceptible to cyber-surveillance offenses. The Union has embarked on initiatives to strengthen capacities, availing crucial training and tools to bolster cyber-defence mechanisms in these regions[10].

3.4 Actions by the EU and Member States

The reinforced export control strategy of the EU has led to some decisive actions, as follows:

- The Union enacted a tight control on the export of facial recognition technologies to China, prompted by pressing concerns over potential human rights violations[11].
- In light of compelling evidence that Belarus used cyber-surveillance to erode democratic principles, curtail civil liberties, intensify domestic oppression, and support Russia's aggressive actions in Ukraine, the EU firmly limited the export of such technologies to Belarus[12].
- Member states play a vital role in the enforcement of the provisions in article 5 of the Regulation. In Germany, prosecutors in Munich have indicted four individuals for the sale of surveillance software to the Turkish government without authorization from the German authorities.

3.5 Conclusion

The EU's commitment to shaping the trajectory of cyber-surveillance exports in a responsible manner serves as a beacon for other global stakeholders. The approach of the EU underscores the belief that technological progress need not come at the expense of human rights or democratic integrity. As other nations grapple with similar challenges, the EU model offers both inspiration and a practical roadmap for action.

4 Third country approaches

4.1 United States

The United States maintains a comprehensive approach to dual-use technology and cyberware through a combination of regulatory measures and international cooperation. While the Wassenaar Agreement plays a pivotal role in regulating the export of dual-use technologies, its effectiveness has faced challenges considering Russia's membership and the evolving geopolitical landscape.

The Wassenaar Arrangement is a multilateral export control regime aimed at preventing the proliferation of dual-use goods and technologies, particularly those with military applications. Yet, the consensus-based membership structure has raised concerns about its efficacy. The US has expressed reservations regarding Russia's adherence to the pact, citing its involvement in cyberattacks and attempts to acquire sensitive technologies.

[10] European Cybercrime Centre – EC3 | Europol, Europol, n.d., https://www.europol.europa.eu/about-europol/european-cyber-crime-centre-ec3.
[11] Laurens Cerulus, 'Europe to Crack down on Surveillance Software Exports,' POLITICO, October 17, 2020, https://www.politico.eu/article/europe-to-curtail-spyware-exports-to-authoritarian-countries/; and, Jakob Hanke Vela and Barbara Moens, 'EU Looks to Ban Companies from Making Sensitive Tech in China,' POLITICO, June 20, 2023, https://www.politico.eu/article/eu-ban-companies-make-sensitive-tech-china/; see, Regulation (EU) 2021/821 of the European Parliament and the Council of 20 May 2021 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items (recast) preamble.
[12] Council Regulation (EU) 2022/328 of 25 February 2022 amending Regulation (EU) No 833/2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine.

The US collaborates closely with the EU on dual-use and cyber-surveillance matters. The Trade and Technology Council (TTC) serves as a forum for such cooperation. It facilitates the alignment of export control regulations, the sharing of threat intelligence, and joint efforts to strengthen cybersecurity.

Both the EU and US work together to harmonize export control regulations, bolster cyber-surveillance capabilities, and address emerging threats. This includes coordinated sanctions on entities involved in cyberattacks and the promotion of responsible behaviour in cyberspace. However, the effectiveness of these collaborative initiatives faces challenges, such as differing regulatory frameworks between the US and the EU, as well as the complicated task of balancing national security interests with economic considerations.

In summary, the US employs a multifaceted approach to dual-use technology and cyberware, but the effectiveness of these measures is complicated by Russia's Wassenaar Agreement membership. EU-US cooperation strives to overcome these challenges, but achieving consensus and striking the right balance remains a complex endeavour. There is a risk that the US will turn to individual Member States if it cannot find a consensus with the EU as a whole as shown by the recent national controls unilaterally established by the Dutch government on the export of semiconductor manufacturing equipment, which were triggered by an agreement between the US, Japan and the Netherlands.

4.2 Japan

Export control measures to counter human rights violations have not yet been legislated in Japan as of August 2023. This topic has been discussed in the security trade control committee led by the Ministry of Economy, Trade and Industry (METI). The last report from the committee was published in June 2021, where it was stated that the legislation for such export control measures has to be considered given that other countries, especially the US and the EU, have already implemented such export control measures, while companies in Japan are potentially still shipping cyber-surveillance items to parties with human rights concerns due to the lack of equivalent measures. However, the concrete approach towards such legislation efforts was not clarified in this report.

Meanwhile, Japan has endorsed the Code of Conduct for Enhancing Export Controls of Goods and Technology That Could be Misused and Lead to Serious Violations or Abuses of Human Rights[13]. This has been established in the context of the Export Controls and Human Rights Initiative[14] launched at the Summit for Democracy[15] with the US taking the lead. By this endorsement, Japan has committed to implementing export control measures to counter human rights violations toward 24 countries[16] that have also endorsed the Code of Conduct.

Considering these developments, it is likely that Japan will legislate export control measures to counter human rights violations in the coming years, but again, the concrete approach towards such legislation has yet to be seen.

[13] Code of Conduct for Enhancing Export Controls of Goods and Technology That Could be Misused and Lead to Serious Violations or Abuses of Human Rights https://www.state.gov/wp-content/uploads/2023/03/230303-Updated-ECHRI-Code-of-Conduct-FINAL.pdf

[14] Fact Sheet: Export Controls and Human Rights Initiative Launched at the Summit for Democracy https://www.whitehouse.gov/briefing-room/statements-releases/2021/12/10/fact-sheet-export-controls-and-human-rights-initiative-launched-at-the-summit-for-democracy/

[15] Democracy cohorts – https://summit4democracy.org/

[16] Albania, Australia, Bulgaria, Canada, Costa Rica, Croatia, Czechia, Denmark, Ecuador, Estonia, Finland, France, Germany, Kosovo, Latvia, The Netherlands, New Zealand, North Macedonia, Norway, Republic of Korea, Slovakia, Spain, and the United Kingdom.

4.3 United Kingdom

Following its exit from the EU, the UK kept the provisions of the EU Dual-use Regulation in its domestic legislation (as 'retained law') applicable in England, Wales and Scotland (Great Britain). However, the updates introduced by EU Regulation 2021/821 have not been retained. Note that the EU Dual-use Regulation, including the 2021 recast, still applies in full in Northern Ireland pursuant to the EU-UK Northern Ireland Protocol of 31/01/2020.

The regulatory framework is the Export Control Act 2002 and the Export Control Order 2008 as amended, both of which contain provisions on UK Security and Human Rights and which apply to cyber-surveillance. Also relevant for cyber-surveillance is the Anti-terrorism, Crime and Security Act of 2001 as amended and the Global Human Rights Sanctions Regulations of June 2020.

The UK maintains its own consolidated list of strategic military and dual-use items that require export authorisation. Like in the EU, the list is derived from both the Wassenaar List of Dual-use items and the Munitions List and contains some extra, national controls especially regarding goods for torture and radioactive sources. The part on dual-use contains the same entries relating to cyber-surveillance as in the EU. On 17 October 2023, the UK issued a technical guidance document in relation to items that could be used to intercept and monitor communications and which are prohibited for export under the UK sanctions on Russia, Belarus, Myanmar, Iran, Syria and Venezuela[17].

4.4 NATO

At the 2021 NATO summit in Brussels a new Comprehensive Cyber Defence Policy was endorsed by the Allies in response to an increase in cyber-attacks by foreign entities and in 2023 NATO launched Virtual Cyber Incident Support Capability (VCISC) to support national mitigation efforts. NATO works with the EU and the OSCE on cyber-defence.

5 Conclusions and recommendations

5.1 Conclusions

The EU Dual-use Regulation (EU) 2021/821 which is a recast of Council Regulation (EC) 428/2009 aims to modernise the EU export control regime to remain in step with international developments. The dual-use Regulation aligns concepts such as export and exporter with those in the Union Customs Code and puts more responsibility and accountability on exporters of dual-use items.

Regulation 2021/821 has broadened the scope of export controls and defines a new category of dual-use items, namely 'cyber-surveillance items' which were added to the list of dual-use items in Annex I of the Regulation. Furthermore, in its article 5 the Regulation introduces a catch-all clause which makes the export of cyber-surveillance items not listed in Annex I subject to export authorisation. The reason behind it is that cyber-technologies are advancing in such a fast pace that they cannot be timely captured by the dual-use Regulation. Another reason resides in the fact that in the dual-use list control levels are determined by technical parameters which are not always applicable to cyber-surveillance items that are defined by their capability for 'surveillance' and are assessed in connection with human rights, internal repression or international humanitarian law. The EU leaves it up to Member States to detect and control the export of newly developed cyber-surveillance items and places part of the burden on exporters which are required to do their own due diligence, to assess the intended end use of their products and to notify their authorities when they suspect misuse.

[17] https://www.gov.uk/government/publications/interception-and-monitoring-prohibitions-in-sanctions-technical-guidance#full-publication-update-history

Countries such as the UK and the US have implemented similar controls on cyber-surveillance items as the EU and are actively enforcing these controls. In the framework of the Summit for Democracy with the US, Japan is taking regulatory action to put in place cyber controls.

In response to rising international tensions, the EU together with allies like the UK and the US has stepped up its sanctions regimes against Russia, Belarus and other countries that serve as hubs to circumvent sanctions. Since the invasion of Ukraine by Russia in February 2022, the EU has issued 11 sanctions packages, which among others prohibit the direct or indirect export to Russia of dual-use items listed in Annex I of the EU Dual-use Regulation. In addition, technologically advanced items as listed in Annex VII to the sanctions Regulation 833/2014 are also prohibited from export to Russia.

It must be noted that the EU is not always aligned with its allies when it comes to sanctions. With respect to China, the US and Japan imposed restrictions on exports of advanced semiconductor manufacturing equipment to China. The EU did not follow these sanctions, but the Netherlands did at their national level which may have repercussions for the internal market.

5.2 Recommendations

The catch-all provision in Article 5 of the Dual-use Regulation mandates that exporters notify their authorities if, based on their due diligence, they are 'aware' that their cyber-surveillance item might be used, either fully or partially, for purposes related to internal repression or significant breaches of human rights and international humanitarian law. The term 'aware' is somewhat ambiguous, and although the Commission has made a good effort in providing guidance on what is expected from exporters in this respect, exporters are still faced with the burden to perform a due diligence for each individual transaction. Some simplifications or streamlining in case of repetitive transactions to certain destinations and end-users should be considered.

Another potential issue is that authorities in different Member States may have a different interpretation of potential human rights abuses or internal repression. That is especially affecting multinational companies operating in several Member States. Uniform decision criteria applied by all Member States should be established.

There should also be uniform guidelines regarding the notification procedure towards the authorities and what information is to be provided and at what time.

6 Bibliography

ECHRI Code of conduct – final – U.S. department of State. Available at: https://www.state.gov/wp-content/uploads/2023/03/230303-Updated-ECHRI-Code-of-Conduct-FINAL.pdf (accessed: 17 October 2023).

Cerulus, L. (2020) *Europe to crack down on surveillance software exports*, *POLITICO*. Available at: https://www.politico.eu/article/europe-to-curtail-spyware-exports-to-authoritarian-countries (accessed: 17 October 2023).

Council Regulation (EU) No 833/2014 of 31 July 2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine EUR-Lex. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.229.01.0001.01.ENG (accessed: 17 October 2023).

Cybercrime center (2023) *Europol*. Available at: https://www.europol.europa.eu/crime-areas-and-statistics/crime-areas/cybercrime (accessed: 17 October 2023).

Democracy cohorts (2023) *Summit for Democracy*. Available at: https://summit4democracy.org/democracy-cohorts-2/ (accessed: 17 October 2023).

Fact sheet: Export controls and human rights initiative launched at the Summit for Democracy (2021) *The White House*. Available at: https://www.whitehouse.gov/briefing-room/statements-releases/2021/12/10/fact-sheet-export-controls-and-human-rights-initiative-launched-at-the-summit-for-democracy/ (accessed: 17 October 2023).

Frequently asked questions – sanctions against Russia (no date) *European Commission*. Available at: https://finance.ec.europa.eu/eu-and-world/sanctions-restrictive-measures/sanctions-adopted-following-russias-military-aggression-against-ukraine/frequently-asked-questions-sanctions-against-russia_en (accessed: 17 October 2023).

Human Rights & Democracy (2021) *EEAS – Europeab Union*. Available at: https://www.eeas.europa.eu/eeas/human-rights-democracy_en (accessed: 17 October 2023).

Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items (recast) (2021) *EUR-lex*. Available at: https://eur-lex.europa.eu/eli/reg/2021/821/oj (accessed: 17 October 2023).

Vela, J. H. and Moens, B. (2023) *EU looks to ban companies from making Sensitive Tech in China*, *POLITICO*. Available at: https://www.politico.eu/article/eu-ban-companies-make-sensitive-tech-china/ (accessed: 17 October 2023).

THE WASSENAAR ARRANGEMENT On Export Controls for Conventional Arms and Dual-Use Goods and Technologies (no date) *The Wassenaar Arrangement*. Available at: https://www.wassenaar.org/ (accessed: 17 October 2023).

'PUBLIC CONSULTATION GUIDELINES ON THE EXPORT OF CYBER-SURVEILLANCE ITEMS UNDER ARTICLE 5 OF REGULATION (EU) No 2021/821' (2023).

PE 754.439
EP/EXPO/INTA/FWC/2019-01/LOT5/1/C/21

Print ISBN 978-92-848-1396-4 | doi: 10.2861/812217 | QA-09-23-562-EN-C
PDF ISBN 978-92-848-1395-7 | doi: 10.2861/415838 | QA-09-23-562-EN-N